UNITED STATES DISTRICT COURT

WESTERN DISTRICT OF WASHINGTON

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. 2:11-cr-00070-RAJ
	)	
	)	
vs.	)	Seattle, WA
	)	
ROMAN V. SELEZNEV,	)	
	)	Jury Trial, Day 8
Defendant.	)	August 24, 2016

VERBATIM REPORT OF PROCEEDINGS
BEFORE THE HONORABLE JUDGE RICHARD A. JONES
UNITED STATES DISTRICT COURT

APPEARANCES:

FOR THE PLAINTIFF: NORMAN McINTOSH BARBOSA
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
norman.barbosa@usdoj.gov

C. SETH WILKINSON
U.S. Attorney's Office
700 Stewart Street, Suite 5220
Seattle, WA 98101-1271
seth.wilkinson@usdoj.gov

HAROLD W. CHUN
U.S. Department of Justice
1301 New York Avenue NW, Suite 600
Washington, DC 20005
harold.chun@usdoj.gov

FOR THE DEFENDANT: JOHN HENRY BROWNE
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
johnhenry@jhblawyer.com

EMMA SCANLAN
Law Office of John Henry Browne
108 South Washington Street, Suite 200
Seattle, WA 98104
emma@jhblawyer.com

Andrea Ramirez, CRR, RPR
Official Court Reporter
United States District Court
Western District of Washington
700 Stewart Street, Suite 17205
Seattle, WA 98101
andrea_ramirez@wawd.uscourts.gov

Reported by stenotype, transcribed by computer

I N D E X

THE CLERK: We are resuming our jury trial in the matter of the United States vs. Roman Seleznev, Cause Number CR11-70, assigned to this court.

THE COURT: Good morning, ladies and gentlemen of the jury.

Each of you should have in your possession now a copy of the Court's final jury instructions. These are your instructions. Feel free to mark them up in any way that you believe appropriate. You can underline them. You can circle particular juror numbers [sic]. The lawyers may make reference to juror numbers -- to jury instruction numbers. So again, you're free to take these home, as well. So when you're educating other people about your experiences as a juror, you'll have these to share with the experience.

So with that, I'd ask that you follow along with me, now, as I read the jury instructions.

Members of the jury, now that you have heard all of the evidence, it is my duty to instruct you on the law that applies to this case. A copy of these instructions will be available in the jury room for you to consult.

It is your duty to weigh and to evaluate all the evidence received in the case, and in that process to decide the facts. It is also your duty to apply the law as I give it to you to the facts as you find them, whether you agree with the law or not. You must decide the case solely on the evidence and the

law, and must not be influenced by any personal likes or dislikes, opinions, prejudices, or sympathy. You will recall that you took an oath promising to do so at the beginning of the case.

You must follow all these instructions and not single out some and ignore others. They are all important. Please do not read into these instructions, or into anything I may have said or done, any suggestion as to what verdict you should return. That is a matter entirely up to you.

A defendant in a criminal case has a constitutional right not to testify. You may not draw any inference of any kind from the fact that the defendant did not testify.

Proof beyond a reasonable doubt is proof that leaves you firmly convinced the defendant is guilty. It is not required that the government prove guilt beyond all possible doubt.

A reasonable doubt is a doubt based upon reason and common sense, and is not based purely on speculation. It may arise from a careful and impartial consideration of all the evidence, or from lack of evidence.

If after a careful and impartial consideration of all the evidence, you are not convinced beyond a reasonable doubt that the defendant is guilty, it is your duty to find the defendant not guilty. On the other hand, if after a careful and impartial consideration of all the evidence, you are convinced beyond a reasonable doubt that the defendant is guilty, it is

your duty to find the defendant guilty.

The evidence you are to consider in deciding what the facts are consists of: One, the sworn testimony of any witness; two, the exhibits received in evidence; and three, any facts to which the parties have agreed.

In reaching your verdict you may consider only the testimony and exhibits received in evidence. The following things are not evidence, and you may not consider them in deciding what the facts are:

1) Opinions, statements, objections, and arguments by the lawyers are not evidence. The lawyers are not witnesses. Although you must consider a lawyer's questions to understand the answers of a witness, the lawyer's questions are not evidence. Similarly, what the lawyers have said in their opening statements, closing arguments, and at other times is intended to help you interpret the evidence, but it is not evidence. If the facts as you remember them differ from the way the lawyers state them, your memory of them controls.

2) Any testimony that I have excluded, stricken, or instructed you to disregard is not evidence. In addition, some evidence was received only for a limited purpose. When I have instructed you to consider evidence in a limited way, you must do so.

3) Anything you may have seen or heard when the Court was not in session is not evidence. You are to decide the case

solely on the evidence received at the trial.

Evidence may be direct or circumstantial. Direct evidence is direct proof of a fact, such as testimony by a witness about what that witness personally saw or heard or did. Circumstantial evidence is indirect evidence; that is, it is proof of one or more facts from which you could find another fact.

You are to consider both direct and circumstantial evidence. Either can be used to prove any fact. The law makes no distinction between the weight to be given to either direct or circumstantial evidence. It is for you to decide how much weight to give to any evidence.

In deciding the facts in this case, you may have to decide which testimony to believe and which testimony not to believe. You may believe everything a witness says, or part of it, or none of it.

In considering the testimony of any witness, you may take into account: One, the witness's opportunity and ability to see or hear or know the things testified to; two, the witness's memory; three, the witness's manner while testifying; four, the witness's interest in the outcome of the case, if any; five, the witness's bias or prejudice, if any; six, whether other evidence contradicted the witness's testimony; seven, the reasonableness of the witness's testimony in light of all the evidence; and eight, any other factors that bear on

believability.

The weight of the evidence as to a fact does not necessarily depend on the number of witnesses who testify. What is important is how believable the witnesses were and how much weight you think their testimony deserves.

A separate crime is charged against the defendant in each count. You must decide each count separately. Your verdict on one count should not control your verdict on any other count.

You are here only to determine whether the defendant is guilty or not guilty of the charges in the indictment. The defendant is not on trial for any conduct or offense not charged in the indictment.

Translations of Russian documents have been admitted into evidence in this trial. Whether the translations are accurate translations of the non-English portions of the documents, in whole or part, is for you to decide based on the evidence presented to you. In considering whether a translation accurately describes the meaning of the document, you should consider any testimony presented to you regarding how and by whom the translation was made, as well as any testimony disputing the translation of any words in the translation. You may consider the knowledge, training, and experience of the translator, if called as a witness.

Although some of you may speak the Russian language, it is important that all jurors consider the same evidence.

Therefore, you should not consider your own understanding of the Russian language in evaluating the accuracy of the translation admitted into evidence.

The indictment charges that the offenses alleged in Counts 1 through 40 were committed on or about a certain day.

Although it is necessary for the government to prove beyond a reasonable doubt that the offenses were committed on a date reasonably near the dates alleged in the indictment, it is not necessary for the government to prove that the offenses were committed precisely on the dates charged.

During the trial, certain charts and summaries were shown to you in order to help explain the evidence in the case. Those charts and summaries were not admitted in evidence, will not go into the jury room with you. They are not themselves evidence or proof of any facts. If they do not correctly reflect the facts or figures shown by the evidence in the case, you should disregard these charts and summaries, and determine the facts from the underlying evidence.

Other charts and summaries have been admitted in evidence. These charts and summaries are only as good as the underlying supporting material. You should, therefore, give them only such weight as you think the underlying material deserves.

You have heard testimony from various witnesses who testified to opinions, and the reasons for their opinions. This opinion testimony is allowed because of the education or

experience of this witness. Such opinion testimony should be judged just like other testimony. You may accept it or reject it, and give it as much weight as you think it deserves, considering the witness's education and experience, the reasons given for the opinion, and all the other evidence in the case.

You have heard testimony from witnesses who testified to both facts and opinions and the reasons for those opinions.

Fact testimony is based on what the witness saw, heard, or did. Opinion testimony is based on the education or experience of the witness.

As to the testimony about facts, it is your job to decide which testimony to believe and which testimony not to believe. You may believe everything a witness says, or part of it, or none of it. Take into account the factors discussed earlier in these instructions that were provided to assist you in weighing the credibility of witnesses.

As to the testimony about the witness's opinion, this opinion testimony is allowed because of the education and experience of this witness. Opinion testimony should be judged just like other testimony. You may accept it, all of it, part of it, or none of it. You should give it as much weight as you think it deserves, considering the witness's education and experience, the reasons given for the opinion, and all the other evidence in the case.

The defendant is charged in Counts 1 through 11 of the

indictment with wire fraud. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly participated in or devised a scheme or plan to defraud, or a scheme or plan for obtaining money or property by means of false or fraudulent pretenses, representations, or promises;

Second, the statements made or facts omitted as part of this scheme were material; that is, they had a natural tendency to influence, or were capable of influencing, a person to part with money or property;

Third, the defendant acted with the intent to defraud; that is, the intent to deceive or cheat;

Fourth, the defendant transmitted, or caused to be transmitted, by wire communication in interstate or foreign commerce, writings, signs, or signals to carry out or attempt to carry out an essential part of the scheme. A wire communication is in interstate or foreign commerce if it goes across a state line or national border.

In determining whether a scheme to defraud exists, you may consider not only the defendant's words and statements, but also the circumstances in which they are used as a whole.

A wire transmission is caused when one knows that the wire transmission will be used in the ordinary course of business, or when one can reasonably foresee such use.

The following chart sets forth the dates of the alleged acts of wire fraud. You may refer to this chart during your deliberations.

Count 1: Date, August 6, 2010; transmission of malware outside the state of Washington to a computer belonging to Mad Pizza, Madison Park, in Seattle, Washington.

Count 2: Date, August 7, 2010; transmission of malware from outside the state of Washington to a computer belonging to Mad Pizza, First Hill, in Seattle, Washington.

Count 3: August 9, 2010; transmission of malware from outside the state of Washington to a computer belonging to Casa Mia Italian Pizzeria Restaurant, in Yelm, Washington.

Count 4: August 28, 2010; transmission of malware from outside the state of Washington to a computer belonging to Mad Pizza, South Lake Union, in Seattle, Washington.

Count 5: October 4, 2010; transmission of malware from outside the state of Washington to a computer belonging to Grand Central Baking Company, in Seattle, Washington.

Count 6: October 22, 2010; transmission of malware from outside the state of Washington to a computer belonging to Broadway Grill, in Seattle, Washington.

Count 7: November 2, 2010; transmission of malware from outside the state of Washington to a computer belonging to Mad Pizza Starfire, in Tukwila, Washington.

Count 8: December 15, 2010; transmission of malware from

outside the state of Washington to a computer belonging to Mad Pizza, South Lake Union, in Seattle, Washington.

Count 9: December 23, 2010; transmission of stolen credit card data from Village Pizza, in Anacortes, Washington, to a server controlled by defendant outside the state of Washington.

Count 10: January 10, 2011; transmission of stolen credit card data from Mad Pizza Starfire, in Tukwila, Washington, to a server controlled by the defendant outside the state of Washington.

Count 11: October 26, 2013; transmission of malware from outside the state of Washington to a computer belonging to Red Pepper Pizzeria, in Duvall, Washington.

An intent to defraud is an intent to deceive or cheat.

An act is done knowingly if the defendant is aware of the act and does not act through ignorance, mistake, or accident. The government is not required to prove that the defendant knew that his acts or omissions were unlawful. You may consider evidence of the defendant's words, acts, or omissions, along with all the other evidence, in deciding whether the defendant acted knowingly.

The jury may find the term "financial institution" in the verdict form. The term "financial institution" means: One, an insured depository institution of the Federal Deposit Insurance Act; or two, a credit union with accounts insured by the National Credit Union Share Insurance Fund.

A defendant's act of wire fraud affects a financial institution if his or her acts of wire fraud caused a new or increased risk of loss to the financial institution.

If you decide that defendant was a member of a scheme to defraud, and that the defendant had the intent to defraud, the defendant may be responsible for other co-schemers' actions during the course of and in furtherance of the scheme, even if the defendant did not know what they said or did.

For the defendant to be found guilty of the offense committed by a co-schemer in furtherance of the scheme, the offense must be one that the defendant could reasonably foresee as a necessary and natural consequence of the scheme to defraud.

The defendant is charged in Counts 12 through 20 of the indictment with intentional damage to a protected computer. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly caused the transmission of a program, information, code, or command to a computer;

Second, as a result of the transmission, the defendant intentionally impaired, without authorization, the integrity of a program, system, or information;

And third, the computer was used in or affected interstate or foreign commerce or communication.

The following chart sets forth the dates of the alleged acts of damage to a protected computer. You may refer to this chart during your deliberations.

Count 12: Date, August 6, 2010; Mad Pizza, Madison Park, Seattle.

Count 13: August 7, 2010; Mad Pizza, First Hill, Seattle.

Count 14: Date, August 9, 2010; Casa Mia Italian Pizzeria Restaurant, in Yelm.

Count 15: August 28, 2010; Mad Pizza, South Lake Union, Seattle.

Count 16: September 13, 2010; Village Pizza, in Anacortes.

Count 17: October 4, 2010; Grand Central Baking Company, Seattle.

Count 18: October 22, 2010; Broadway Grill, Seattle.

Count 19: November 2, 2010; Mad Pizza Starfire, in Tukwila.

Count 20: October 26, 2013; Red Pepper Pizzeria, in Duvall.

The defendant is charged in Counts 21 through 29 of the indictment with unlawfully obtaining information from a protected computer without authorization. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt: First, the defendant intentionally accessed without

authorization a computer; and second, by accessing without authorization a computer, the defendant obtained information from a computer that was used in or affected commerce or communication between one state and other states, or between a state of the United States and a foreign country.

The following chart sets forth the dates of the alleged acts of unlawfully accessing a protected computer. You may refer to this chart during your deliberations.

Count 21: August 6, 2010; Mad Pizza, Madison Park, Seattle.

Count 22: August 7, 2010 -- let me begin again.

Count 21: Beginning date is August 6, 2010. End date is 2/15/2011. That's Mad Pizza, Madison Park, Seattle.

Count 22: Beginning date is August 7, 2010. Ending date is February 15, 2011. That's Mad Pizza, First Hill, Seattle.

Count 23: Beginning date is August 9, 2010, to February 23, 2011; Casa Mia Italian Pizzeria Restaurant, in Yelm.

Count 24: August 28, 2010, through February 1, 2011; Mad Pizza, South Lake Union, Seattle.

Count 25: September 13, 2010, through March 26, 2011; Village Pizza, Anacortes.

Count 26: October 4, 2010, through December 1, 2010; Grand Central Baking Company, Seattle.

Count 27: October 22, 2010, through October 27, 2010;

Broadway Grill, in Seattle.

Count 28: November 2, 2010, to February 1, 2011; Mad Pizza Starfire, Tukwila.

Count 29: October 26, 2013, through May 1, 2014; Red Pepper Pizzeria, in Duvall.

The defendant is charged in Counts 30 to 38 of the indictment with possession of 15 or more unauthorized access devices. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly possessed at least 15 unauthorized access device at the same time;

Second, the defendant knew that the devices were unauthorized;

Third, the defendant acted with the intent to defraud;

And fourth, the defendant's conduct in some way affected commerce between one state and other states, or between a state of the United States and a foreign country.

An unauthorized access device is any device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

The following chart sets forth the dates of the alleged possession of access devices for each victim. You may refer to this chart during your deliberations.

Count 30: The date is August 6, 2010; Mad Pizza, Madison

Park, Seattle.

Count 31: August 7, 2010; Mad Pizza, First Hill, Seattle.

Count 32: August 9, 2010; Casa Mia Italian Pizzeria Restaurant, in Yelm.

Count 33: August 28, 2010; Mad Pizza, South Lake Union, Seattle.

Count 34: September 13, 2010; Village Pizza, in Anacortes.

Count 35: October 4, 2010; Grand Central Baking Company, Seattle.

Count 36: October 22, 2010; Broadway Grill, Seattle.

Count 37: November 2, 2010; Mad Pizza Starfire, Tukwila.

Count 38: October 26, 2013; Red Pepper Pizzeria, in Duvall.

An access device means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access, that can be used alone or in conjunction with another access device to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.

A credit card number is an access device.

A person has possession of something if the person knows of its presence and has physical control of it, or knows of its

presence and has the power and intention to control it.

More than one person can be in possession of something if each knows of its presence and has the power and intention to control it.

The defendant is charged in Counts 39 and 40 of the indictment with aggravated identity theft. In order for the defendant to be found guilty of that charge, the government must prove each of the following elements beyond a reasonable doubt:

First, the defendant knowingly transferred, possessed, or used without legal authority a means of identification of another person;

Second, the defendant knew that the means of identification belonged to a real person;

And third, the defendant did so during and in relation to the crime of wire fraud or possession of 15 or more unauthorized access devices.

An access device, as defined in Instruction Number 25, is a means of identification.

Count 39 charges the defendant with aggravated identity theft in connection with a credit card number ending in the digits 5719, belonging to a person with the initials D.K.

Count 40 charges the defendant with aggravated identity theft in connection with a credit card number ending with the digits 2897, belonging to a person with the initials R.G.

A defendant may be found guilty of wire fraud, intentional damage to a computer, obtaining information from a computer without authorization, possession of 15 or more unauthorized access devices, or aggravated identity theft, even if the defendant personally did not commit the act or acts constituting the crime, but aided and abetted in its commission. To prove a defendant guilty of aiding and abetting, the government must prove beyond a reasonable doubt:

First, the crime of wire fraud, intentional damage to a computer, obtaining information from a computer without authorization, possession of 15 or more unauthorized access devices, or aggravated identity theft was committed by someone;

Second, the defendant aided, counseled, commanded, induced, or procured that person with respect to at least one element of the crime;

Third, the defendant acted with the intent to facilitate the crime;

And fourth, the defendant acted before the crime was completed.

It is not enough that the defendant merely associated with the person committing the crime, or unknowingly or unintentionally did things that were helpful to that person, or was present at the scene of the crime. The evidence must show beyond a reasonable doubt that the defendant acted with the knowledge and intention of helping that person commit wire

fraud, intentional damage to a computer, obtaining information from a computer without authorization, possession of 15 or more unauthorized access devices, or aggravated identity theft.

A defendant acts with the intent to facilitate the crime when the defendant actively participates in a criminal venture with advance knowledge of the crime and having acquired that knowledge when the defendant had a realistic opportunity to withdraw from the crime.

When you begin your deliberations, elect one member of the jury as your foreperson, who will preside over the deliberations and speak for you here in court.

You will then discuss the case with your fellow jurors and reach agreement, if you can do so. Your verdict, whether guilty or not guilty, must be unanimous.

Each of you must decide the case for yourself, but you should do so only after you have considered all of the evidence, discussed it fully with the other jurors, and listened to the views of your fellow jurors.

Do not be afraid to change your opinion if the discussion persuades you that you should. But do not come to a decision simply because other jurors think that it is right.

It is important that you attempt to reach a unanimous verdict, but, of course, only if each of you can do so after having made your own conscientious decision. Do not change an honest belief about the weight or effect of the evidence simply

to reach a verdict.

Because you must base your verdict only on the evidence received in the case and on these instructions, I remind you that you must not be exposed to any other information about the case or to the issues it involves. Except for discussing the case with your fellow jurors during your deliberations, do not communicate with anyone in any way, and do not let anyone else communicate with you in any way about the merits of the case or anything to do with it. This includes discussing the case in person, in writing, by phone or electronic means, via e-mail, text messaging, or any internet chat room, blog, website, or other feature. This applies to communicating with your family members, your employer, media or press, and the people involved. If you are asked or approached in any way about your jury service or anything about this case, you must respond that you've been ordered not to discuss the matter, and to report the contact to the Court.

Do not read, watch, or listen to any news or media accounts or commentary about the case, or anything to do with it. Do not do any research, such as consulting dictionaries, searching the internet, or using any reference materials. And do not make any investigation or in any other way try to learn about the case on your own.

The law requires these restrictions to ensure the parties have a fair trial based upon the same evidence that each party

had an opportunity to address. A juror who violates these restrictions jeopardizes the fairness of these proceedings, and a mistrial could result that would result in the entire trial process to start over. If any juror is exposed to any outside information, please notify the Court immediately.

Some of you have taken notes during the trial. Whether or not you took notes, you should rely on your own memory of what was said. Notes are only to assist your memory. You should not be overly influenced by your notes or those of your fellow jurors.

The punishment provided by law for this crime is for the Court to decide. You may not consider punishment in deciding whether the government has proved its case against the defendant beyond a reasonable doubt.

A verdict form has been prepared for you. After you reach unanimous agreement on a verdict, your foreperson should complete the verdict form, according to your deliberations, sign and date it, and advise the courtroom deputy that you're ready to return to the courtroom.

If it becomes necessary during your deliberations for you to communicate with me, you may send a note through the courtroom deputy, signed by any one of you, or more. No member of the jury should ever attempt to communicate with me except by a signed writing, and I will respond to the jury concerning the case only in writing, or here in open court.

If you send out a question, I will consult with the lawyers before answering it, which may take some time. You may continue your deliberations while waiting for the answer to any question. Remember that you're not to tell anyone, including me, how the jury stands, numerically or otherwise, on any question submitted to you, including the question of the guilt of the defendant, until after you've reached a unanimous verdict or have been discharged.

Members of the jury, if you'd like to stand and stretch at this time, please do so.

Please be seated.

Ladies and gentlemen of the jury, I now ask you to give your undivided attention to Mr. Barbosa, who represents the United States, as he gives his closing remarks.

Counsel, you may proceed.

MR. BARBOSA: Thank you, Your Honor.

1.7 million credit cards, folks. 1,700,000 credit card tracks; those stolen credit card numbers, along with U.S. federal court criminal record searches for defendant's true name and his hidden names, bulba and 2Pac, two days before he was caught in the Maldives; and his password cheat sheet with the logins and passwords, the credentials for his entire criminal underground infrastructure, those are the credentials he used for the servers to steal credit cards, the credentials for his domains where he sold these credit cards, and his

e-mail accounts used to manage his criminal enterprise, all used for nearly a decade to orchestrate his hacking and credit card trafficking scheme. Those three pieces of evidence were sitting on a laptop computer, this computer, that was in that bag, strapped over his shoulder, when Secret Service agents picked him up in the Maldives.

Those three pieces of evidence, the 1.7 million credit cards, his court record searches, and his password cheat sheet, tell you just about everything you need to know in this case. Those three pieces of evidence alone show that this defendant, Roman Seleznev, was running a massive scheme to hack point-of-sale systems, steal millions of credit cards, and sell those stolen credit cards on underground carding forums and automated vending sites.

And they didn't just magically appear on this laptop. 1.7 million credit cards weren't planted there by some super-hacker. They didn't jump onto this computer over a dead wi-fi connection nearly 7,500 miles away from its last connection in the Maldives. And they sure weren't loaded over a cellular connection that hadn't been used since June 18, when defendant left Moscow for his island vacation. That evidence was on defendant's laptop because he put it there. He was carrying those credit card numbers because he is one of the most prolific credit card traffickers in history. He was carrying those credit card numbers because stolen credit card

track data is his stock in trade.

For nearly a decade, this defendant has been stealing from merchants and banks all over the world, 3,700 different banks, and merchants right here in downtown Seattle, like the Broadway Grill; making tens of millions of dollars running this criminal enterprise, all behind a keyboard in Vladivostok, Russia, and Bali, Indonesia; hiding his true identity behind a series of nics that you heard about over the last several days, that became notorious amongst law enforcement, but truly revered in the underground world of carding.

This defendant was the only trusted vendor on carder.su, one of the world's largest carding forums. And no doubt, as he sat behind that keyboard, he was feeling untouchable, comforted in the knowledge that he couldn't be extradited from Russia to face justice, and hoping that the Maldives, without an extradition treaty, wouldn't turn him over when he went on vacation.

I'm going to spend the next 30 minutes or so talking about how this scheme worked, the law that will guide you when you're deliberating on the charges, and how the evidence that you've seen fits in with those charges. Most of the time, we're going to be talking about the e-mail accounts, the servers, and the domains that you've seen on this infrastructure chart that we've been referring to throughout the trial. And I'm going to spend much of my time talking about how all the evidence in

this case points to one person, the defendant, as the hacker behind these accounts, these servers, and domains, and the keyboard, in the upper left-hand corner, where these attacks were launched.

But before we go into the evidence in more detail, I want to start with a quick review of how this scheme worked. You've heard a flood of evidence over the last several days. It came in in some dense pieces of material, code, and the long testimony from Detective Dunn.

So I want to turn back to this infrastructure chart and talk to you specifically about Counts 1 through 11 of the indictment. Those are the charges of wire fraud affecting a financial institution.

And the wire fraud charges, much like this infrastructure charge, can provide you with a road map to all of the other counts in this case; a road map of the charges of intentional damage to a protected computer, in Counts 12 through 20; obtaining information from a protected computer, in Counts 21 through 29; possession of 15 or more unauthorized access devices, in Counts 30 through 38; and the two counts of aggravated identity theft, in Counts 39 and 40. All of those other counts flow from the wire fraud scheme that is charged in Counts 1 through 11. Because those charges, the wire fraud charges, encompass defendant's entire scheme outlined on this map.

The wire fraud charges describe how, sitting behind the computer in the upper left-hand corner, defendant launched his attacks on victims all over the world; how sitting behind this keyboard in Vladivostok, or Bali, or the Maldives, defendant would launch port scans, looking for vulnerable point-of-sale networks. Those port scans are the scans of wide swaths of the internet that Detective Dunn explained to you, where the defendant would look for a specific open door, a port, 3389, that he knew small businesses all over the world used for remote access to service their point-of-sale systems. He knew this was a vulnerability in their systems that he could attack, using widely known and common passwords from the point-of-sale industry.

From there, the wire fraud charges explain how defendant's scheme involved reaching out to his malware server, in the lower left-hand corner, the "shmak" and "smaus" server, to pull down his malicious code over the internet, over the wires, onto the victims' computers, in the center of the chart. The charges in the wire fraud counts also explain how defendant configured that malware to scoop up all of the credit card data and transmit that data over the internet, again over the wires, to defendant's dump collection servers, over here in the lower right-hand corner.

These dump servers, the Ukraine server, the HopOne server, and even the shmak and smaus server, at times, were the servers

that the defendant rented and configured to receive the stolen data. From there, the wire fraud charges describe how defendant would harvest the numbers, pick them up from his dump collection servers, and post them for sale on his vending sites, track2, and bulba, in the upper right-hand corner of the chart.

Finally, the wire fraud charges describe how defendant did this all with the intent that his customers would use those stolen credit cards at merchants throughout the world, with the intent to defraud the merchants and the issuing banks by falsely claiming that these were legitimate credit cards, that they were authorized to use these credit cards, even though they fully knew that these had been stolen, and weren't authorized.

That's the essence of the wire fraud charges. So let's talk a little bit about the law that should guide you as you deliberate on the charges in this case.

There are a total of 40 counts in this case. And it's a lot. And as the Court has instructed you, it's your job to consider each charge separately. But even though you have to consider all 40 counts separately, there are just five instructions that tell you what you must find in order to convict the defendant of each of the sets of charges. Those instructions set forth the elements of each crime that is charged.

As you go back to the jury room and begin looking over the charts of the charges, generally what you'll find is that there's one count of each crime -- with the exception of the aggravated identify theft, there's one count of each crime, wire fraud, intentional damage to protected computers, obtaining information from a protected computer, and possession of 15 or more unauthorized access devices, from each of the victim businesses that was impacted.

The only exceptions are the wire fraud counts for Mad Pizza Starfire and South Lake Union. There are two counts each of wire fraud for those locations, one for the transmission of the malware to their systems, and one for the transmission of the stolen data back out to one of the dump collection servers.

The instruction that lays out the elements for wire fraud, that you have in your packet of instructions there, is Instruction 16. And I will shorten it a little bit with the instructions that you have there.

And what that provides is that to find the defendant guilty of wire fraud, you need to find the defendant [sic] proved four elements beyond a reasonable doubt:

First, the defendant knowingly participated in or devised a scheme or plan to defraud by means of false statements, pretenses, representations, or promises;

Second, the false statements made as part of the scheme were material, meaning they had a natural tendency to influence

someone to part with money or goods. Presenting a credit card tends to influence the recipient of that credit card to provide you with goods or services.

Third, the defendant acted with the intent to defraud;

And fourth, as part of the scheme, the defendant used the wires in interstate or foreign commerce.

I'm not going to go over each and every one of these elements, but I do want to address a couple issues in this instruction that you may wish to focus on.

First, what does it mean to participate in a scheme and artifice to defraud, and act with the intent to defraud? Well, here it means this defendant participated in a scheme to defraud in which he and his co-schemers, the people buying the stolen credit cards from him, over and over again, intended to fraudulently present those fake credit cards to obtain goods and services, knowing that the credit card numbers were stolen and unauthorized. Keep in mind, defendant doesn't have to be the person standing at the register who used these stolen credit cards.

The Court has also instructed you in Instruction 21 that if you find he was part of this scheme, he was responsible for all of the fraud he intended to help facilitate. And if you have any question about whether he knew what was going on and intended to help facilitate this fraud, the $169 million in fraud losses tied to the cards he stole, or more specifically,

tied only to the cards that were found by law enforcement on the servers they managed to get their hands on, that question is answered by defendant's posdumps website. That question is answered by this self-styled tutorial, where he explains to his customers, step by step, how to "make and use fake credit card." And where he politely reminds them, "Remember, this is illegal way." This is the tutorial where defendant teaches his customers exactly how to use stolen credit cards, commit fraud, where he advertises his dump shop, 2Paccc, and tells his customers how to find the best dumps and make fake credit cards.

And as if that wasn't enough, before he penned that helpful tutorial on how to commit fraud the illegal way, defendant had participated in carding forums like these, carder.su, CardingPlanet, CardingWorld, Omerta, inFrauD, and others, for years. These carding forums are like defendant's virtual clubhouses, where he would hang out with other carders and plan their crimes, share ideas and tools, trade information on how to hack point-of-sale systems, chat about how to commit credit card fraud, and gossip about who has the best dumps. That evidence shows defendant knew exactly what he was doing. He knew exactly what his customers would do with these cards, and it shows he was actively assisting his customers and working with them to commit fraudulent purchases, because he fully intended for them to use the fake cards and come back to

him for more.

What about that fourth element, the requirement the defendant transmitted or caused the transmission of wires in interstate or foreign commerce?

Well, here's the chart that Detective Dunn went over with you when he was testifying about his review of all the victim systems. Each of these arrows represents wire transmissions defendant used, either to plant his malware on a victim system, or wire stolen credit cards from the victim system to one of his dump collection servers. And every one of these wires was in interstate or foreign commerce. Whenever defendant installed his malware on a victim computer, he pulled it down from his malware server in Russia, the shmak or smaus server, up here on the top left corner. Sometimes he sent the stolen numbers back to the same server, like in the case of Schlotzky's Deli, Grand Central Baking, and Mad Pizza, Madison Park, where the arrow is going in both directions, representing the malware coming down and the numbers heading back to the server. Other times, he'd send the stolen data to the Ukraine server or the HopOne server. But in every single instance, whether it was the malware or the stolen numbers, these internet signals were traveling over the wires in either interstate or foreign commerce.

For the specific wire fraud transmissions, you have this chart in Exhibit 1.15 that Detective Dunn prepared. And this

will be back with you in the jury room, and is an exhibit that was admitted.

This chart shows each of the times defendant transmitted malware to one of the victim computers. And it also provides you the IP address and location for the dump collection server the defendant was using. And you'll also find, in the far right column, it gives you a reference to the underlying exhibit, the forensic artifacts and details that Detective Dunn found on those victim systems.

For Counts 9 and 10, which allege the transmission of stolen credit card data from Village Pizza and Mad Pizza Starfire -- not the installation, so this is the other half of the scheme. Most of these are related to installation of malware. But for Counts 9 and 10, you have Detective Dunn's explanation of how that malware operated; that during the entire time that the malware was running on those victim computers, it's transmitting stolen credit cards, daily. So those cards are encompassed in the time period between the installation date and the mitigation date, when law enforcement responds and the scheme is brought to an end.

Once you have found defendant guilty of any particular count of wire fraud, you're also being asked to determine whether each count affected a financial institution. It's somewhat comical in this case. We have thousands of banks involved. But this is why you heard from the National Credit

Union Administration and the Federal Deposit Insurance Corporation, as well as from Ms. Wood. As you heard from them, the scheme unquestionably targeted banks, merchants, 3,700 different banks and over $169 million in losses.

What about the other charges you have to decide on? Well, I told you earlier, the wire fraud charges in the infrastructure chart are a road map to all of these other charges. That's because the other charges, the intentional damage to a protected computer, the obtaining information from a protected computer, possession of stolen credit card, and the aggravated identity theft, they're all separate but equally illegal parts of the wire fraud scheme. To complete this wire fraud scheme, that you see in Counts 1 through 11, defendant took each of the steps that is charged in the other counts.

The intentional damage charges, in Counts 12 through 20, hold him to account for his installation of the malware on the victim systems. The elements of that crime are set forth in Instruction 22. And those elements provide that to find him guilty, first, you have to find that he knowingly transmitted codes or commands to a computer without authorization. Second, as a result of the transmission, he intentionally impaired the integrity of the victim's system or information, specifically, their credit card data. And third, the computer was used in or affected interstate or foreign commerce or communications.

We'll talk about the effect on interstate or foreign

commerce in a minute, because it applies to several of the counts.

But the first two elements of this crime go to the heart of the defendant's scheme. Every time the defendant took his malware and installed it on one of these victim machines, he established the first two elements of that crime, knowingly transmitting code with the intention of impairing the integrity of the system and the data located on it.

For the counts of intentional damage to a protected computer, once you've found the defendant guilty of any one of those counts, you also have a follow-up question. You have to consider whether the offense caused loss to one or more persons, during a one-year period, aggregating $5,000 or more.

You heard from several of the victims in this case. These point-of-sale intrusions cost them thousands and thousands of dollars. For each of them, the combined cost of incident response, private forensic investigations, legal fees, fines from Visa and MasterCard, and the damage to their business reputations cost well over $5,000. When a small business like this is hit by a point-of-sale intrusion, they are on the hook for at least $5,000 to $10,000 in fines, upwards of $20,000 to $30,000 in private forensic investigation costs. And this isn't even counting the damage to their business reputation or the costs like replacing their computers. It's just not seriously debatable that these attacks always caused more than

$5,000 in damages.

The next set of counts is Counts 21 through 29, which charged defendant with obtaining information from a protected computer. And those charges are related to defendant's theft of the credit card data from the victim systems.

The elements of obtaining information from a protected computer are in Instruction 23. And they state that to find the defendant guilty of these counts, you have to find, first, that the defendant intentionally accessed a computer without authorization; second, by accessing the victim's computer, the defendant obtained information; and that the computer was used in or affected interstate or foreign commerce communications. Again, these charges go to the heart of the scheme. Defendant's entire infrastructure was established for the sole purpose of intentionally hacking into these victim systems and obtaining information, information including the millions of stolen credit cards he later sold on his vending site.

You will find that these counts, the obtaining information counts, cover a time period between the installation and the mitigation of the malware. Because any time within that period -- or the entire time within that period defendant is in control of those systems and obtaining information on a regular, rolling basis, numbers rolling in to his dump collection servers through the operation of his malware.

For those counts, again, you have a follow-up question if

you find him guilty. For those counts, you have to decide whether the offense was committed for commercial advantage or private financial gain. And the answer to that question is fairly obvious from the facts. The purpose of this scheme was not charity. The purpose of setting up those Liberty Reserve accounts that received nearly $17 million in proceeds from his credit card sales was private financial gain. It was all designed to line his pockets with the proceeds of these stolen goods.

That brings us to the possession of unauthorized access device charges in Counts 30 through 38. Those charges account for the fact that once he installed his malware on each victim's point-of-sale system, he is then in possession of every credit card number that transits that system, hundreds of credit cards, every day, at every victim he had.

The elements of that crime are in Instruction 24. And they provide that to find defendant guilty of those counts, you must find, first, the defendant knowingly possessed at least 15 unauthorized access devices at the same time; second, the defendant knew that the devices were unauthorized; third, the defendant acted with the intent to defraud; and fourth, the defendant's conduct in some way affected interstate or foreign commerce.

For those counts, the first thing you need to know is that, as the Court has instructed you in Instruction 25, credit

card numbers are access devices. This could be rewritten as unauthorized possession of credit cards. And an unauthorized access device is basically a stolen credit card, or one that was obtained with intent to defraud. And in this case, again, the entire essence of this scheme is defendant's theft of these credit cards with the intent that they be used to commit fraud. So again, these elements just aren't reasonably in dispute.

You also need to note that possession is not limited to physical possession of a card, plastic card. The Court has instructed you, in Instruction 25, that a person has possession of something if the person knows of its presence and has physical control of it, or knows of its presence and has the power and intention to control it.

Here, defendant was planting malware, on each of these victim systems, that gave him complete control over the credit card data on those systems. On any given day, he was in total control of hundreds of credit card numbers for each victim he had. And as a result, he was in possession of 15 or more credit cards.

I skipped over that interstate commerce element for all three of those last ones. Each of these charges, intentional damage to a protected computer, obtaining information from a protected computer, and possession of 15 or more unauthorized access devices, carries this element of an impact on interstate or foreign commerce or communications. This is an element you

see in a lot of federal criminal statutes, and it gives the Court jurisdiction over this case. Each of those crimes requires proof that the crime affected interstate commerce, either because the computers that the defendant hacked were used or affected -- used in or affected interstate or foreign commerce, or the stolen credit cards he possessed in some way affected interstate or foreign commerce.

And in this case, you heard testimony that the computers the defendant hacked, these are small-business point-of-sale systems that are being used to process credit card payments over the internet, from banks all over the country, and from global credit card brands, like American Express, Discover, MasterCard, and Visa. And the credit cards he stole came from banks all over the country, from local credit unions, like BECU, the Seattle Metropolitan credit card -- Credit Union -- all the way up to well-known national banks, JPMorgan Chase, Wells Fargo, Bank of America. And what this tells you is that any business handling credit cards, in this day and age, is connected to interstate or foreign commerce. And as a result, those credit card numbers and the computers that the defendant was attacking are protected under federal law.

Finally, we have the two aggravated identity theft charges. And those are just a couple examples of defendant's possession of the means of identification, the names and credit card numbers, of just two of the millions of people whose

credit cards defendant stole over the years he operated his criminal enterprise.

The elements of aggravated identity theft are in Instruction 27. And they provide that to find the defendant guilty, you must find beyond a reasonable doubt that, first, the defendant knowingly transferred, possessed, or used, without legal authority, a means of identification of another person; second, the defendant knew that the means of identification belonged to a real person; and third, the defendant did so during and in relation to another crime, specifically, here, the wire fraud or the unauthorized possession -- or excuse me -- or the possession of 15 or more unauthorized access devices.

Count 39 is related to defendant's possession of Mr. Knoernschild's name and BECU credit card number. This was the credit card account that Mr. Forsythe, the former BECU security investigator, talked to you about, and introduced in the exhibit from his records the credit card track data that had been stolen from Broadway Grill as part of the counts in the wire fraud. This was one of the first hacks that started Detective Dunn's investigation.

And Count 40 is a bookend to this case. It's related to defendant's possession of Ms. Gebhard's BECU credit card that Agent Fischlin showed you was sitting on defendant's laptop when he was picked up in the Maldives, the one that Agent

Fischlin was able to trace back to Red Pepper Pizzeria and find in the malware log files, sitting on their computer in Duvall, 7,500 miles away.

Speaking of Red Pepper Pizzeria, during Agent Fischlin's cross, defense suggested that you don't have any evidence that the defendant stole the credit card numbers there. This was the hack that was traced directly to defendant's laptop computer. This was the hack that Agent Fischlin only discovered after finding Ms. Gebhard's credit card number sitting in the dump file on defendant's computer, with the title Washington 1000 [sic], and hundreds of credit card numbers with Western Washington zips and cities listed. The attack on Red Pepper Pizzeria used the same remote desktop methodology seen throughout this case.

And if that wasn't enough to convince you that defendant is responsible for the intrusion of Red Pepper Pizzeria, the password he used for the malware at Red Pepper Pizzeria should put that to bed for good. Exhibit 1.10, this is from the artifacts that Agent Fischlin found on the system at Red Pepper. And the password for that malware was "2pacsakur," defendant's hero, his nic at the time that he was picked up in the Maldives. That's defendant's work. That's defendant's signature. He hacked Red Pepper Pizzeria and stole those numbers just as surely as he hacked all the other victims in this case. And that's why the numbers from Red Pepper Pizzeria

were sitting on his computer over 7,500 miles away.

So that's all of the charges in this case. And even though they're all part of the overall wire fraud scheme, each count addresses a separate illegal act by the defendant, and each charge constitutes a separate criminal offense.

So let's talk a little bit about what else is not really in dispute here. Nobody can reasonably dispute that these victims were hacked. And the hacker responsible for stealing all these credit card numbers, they were -- the hacker responsible for that hack was stealing all the credit card numbers. And it's not really debatable that someone launched a series of computer attacks that involved port scanning or open point-of-sale networks. You've seen that evidence repeatedly, in the HopOne servers, with the port scanning tools. You've seen it in the rubensamvelich accounts, with abuse reports recording port scanning.

Nobody can dispute that the shmak and smaus server was planting malware on computers all over the world. You've seen the malware on the victims' computers. That didn't come with those systems. The business owners sure didn't put it there. That malware was put there by the hacker responsible for these crimes. The evidence you saw, the pieces of code that Detective Dunn found on these systems, showed how that malware was sending the stolen credit card numbers out to one of three different servers throughout the course of this scheme.

And no one can reasonably dispute that these vending sites, track2, bulba, and 2Pac, were selling millions of stolen credit cards that trace back to victim merchants in this case. Those sites are criminal on their face. They don't even pretend to be legitimate.

No one can reasonably dispute that all of this activity, the hacking and credit card trafficking, traced to all this cybercrime infrastructure you've seen in the infrastructure chart over the past week and a half, you can't dispute that this caused an enormous financial loss to thousands of banks and merchants all over the country. And the testimony you heard from the victims demonstrates the damages it caused.

The only question you really have to answer in this case is whether the defendant was the man sitting behind the keyboard, responsible for all of this hacking and credit card trafficking. That comes down to the evidence you've seen tying him to each of the nics that he used to run the scheme, each of the pieces of infrastructure on this chart, the e-mail accounts, the domains, and the servers that were used to operate this scheme.

Time and again, that evidence consistently points to just one person, across multiple sources of evidence. It consistently points to the defendant. The defendant is the person behind these nicknames: NCuX, track2, bulba, and 2Pac. These were the nics that the defendant hid behind. These were

the nics that defendant had carefully crafted and cultivated for years to build a reputation as one of the biggest and most reliable sources of credit card data on the internet. But despite his best efforts to hide behind those nics and keep his true identity out of the hands of law enforcement, he slipped up. And he slipped up repeatedly.

At the beginning of the trial, Mr. Wilkinson told you how defendant left traces of his identity, digital fingerprints, all over the crime scene in this case; how defendant left his digital fingerprints on the infrastructure used to run his enterprise, the e-mail accounts, the servers, and the domains that he used to operate this entire scheme. But unlike a physical crime scene, where a defendant may leave a single fingerprint, or maybe a partial fingerprint, Mr. Seleznev left dozens of fingerprints. He left them nearly everywhere he went on the internet.

Before agents even opened up defendant's laptop and found his stash of $1.7 million credit cards, before they discovered his posdumps tutorial and the cheat sheet with the credentials for all his criminal infrastructure, agents had traced every piece of criminal infrastructure we've seen in this case to one person by following defendant's digital fingerprints across the internet. He left them on the dump servers he used to collect stolen goods. As you saw in this exhibit from the HopOne server, where defendant is buying an airplane ticket in his

true name, with his true date of birth, and the passport number from the passport he was carrying when he was caught three years later in the Maldives.

He left them in the e-mail accounts he used to manage his credit card vending sites, like this PayPal receipt that Detective Dunn found in the rubensamvelich account. Remember, the rubensamvelich account is the one used to manage the HopOne server, as well as defendant's vending sites at the track2 domains. And this receipt that Detective Dunn found didn't just have defendant's name. It had defendant's home address, in Vladivostok, that was listed as his primary residence in the passport he was carrying when he was taken into custody in the Maldives.

And the flower orders for his wife and other internet receipts found in the boookscafe account, this is the account that defendant was using to manage the shmak and smaus server, as well as his nCuX domains, earlier in his career. And you'll find in this receipt one of his phone numbers, ending in 5285, the same phone number that shows up on his PayPal records in his true name, Roman Seleznev, as well as on three accounts he opened in one of his fake names, Roman Ivanov, and in the Western Union records when he went to pick up a wire transfer and presented his real passport, again with his real date of birth and the same passport number that matched the one found on him when he was arrested.

Why is it the defendant's name, defendant's date of birth, his passport number, and his phone number, all of his digital fingerprints, not Roman Ivanov, not Romper Stomper, or some man named Alexey Davydov, or any one of defendant's other names? Why is it the defendant's name and true identifiers keeps popping up in all of the places tied to this criminal infrastructure? It's there because these are his accounts. These are his servers and his domains. His name keeps popping up everywhere because he's running this entire show.

But he didn't just leave digital fingerprints on these crime scenes. Unique usernames and passwords are today's digital equivalent of a signature. How many of you have that go-to username and password that you put on random internet sites that you have to go to, and you're sick of trying to come up with a new and unique password for every single internet store you go to? Everyone has them. We're told, "Stop using the same username. Stop using the same password." But they're difficult to remember. Everyone has a go-to username. The defendant tried to use different usernames. But just like everyone else, he gets sick of making up new names and passwords.

A few of defendant's usernames and passwords have been a constant throughout his criminal career on the internet. As you go through the evidence in this case, you may notice that defendant's career as a carder has three chapters. They

correspond to his primary nics, nCuX, track2, bulba, and 2Pac. NCuX generally covers the time period from about 2007 to 2009. Track2 and bulba cover the time period from 2009 through roughly 2012 or early 2013. And 2Pac was the nic that the defendant adopted in 2013 and kept through the date of his arrest.

And while defendant changed those primary nics, the ones he displayed for the world to try to keep distance from his true identity, he consistently used three background or go-to nics and passwords for his back-end accounts, his personal internet browsing, the things he thought were hidden behind his keyboard: Smaus, ochko, shmak. Those are defendant's go-to usernames and passwords that he used to sign the digital crime scenes in this case, over and over again. Those three accounts, especially smaus and ochko123, it's a thread that runs through defendant's entire career. Smaus and ochko123 show up all over this case, and they tie this defendant to the infrastructure he's used since his days as nCuX, back in 2006, all the way through the day of his arrest.

Look at this e-mail in Exhibit 5.15 from the boookscafe account. This is where defendant is talking to one of his customers about his BIN list, when he's still operating as nCuX. And he's telling his customer to check out one of his domains, nCuX.name. If you look towards the bottom of this, you'll notice he's named one of his BIN lists "smausBIN." That

signature, smaus, along with the password ochko123, shows up repeatedly in the boookscafe account for defendant's personal internet accounts.

If you recall, the boookscafe account is an older account. It had been in operation for a long time. It had been opened up in 2006. And defendant began using it as early as 2007, in the name nCuX.

This is Exhibit 16.2. This is the chat with uBuyWeRush. This is where defendant was talking to uBuyWeRush to order one of these, an MSR206, our handy card reader and writer. And you see in this he listed his true name; his true address, same one that shows up in his passport; and the e-mail address boookscafe@yahoo.com, as early as February 2007. Defendant used that boookscafe account for years to run his credit card trafficking enterprise as nCuX, before supposedly retiring in 2009.

He also used that e-mail account, the boookscafe account, to manage the smaus and shmak server. These receipts I have on the screen now, these are from FirstVDS hosting. You can find them in Exhibit 5.11A. They show the defendant managing the smaus server, smaus.fvds.ru. But even though defendant retired his nCuX name, he never retired this server. This is the server where he kept his toolkit. This is the server where he hosted all his malware, the malware that he was pulling down onto the victims' systems.

It's also the first server that Detective Dunn saw in this case. Remember his testimony about going out to Coeur d'Alene, Idaho, in May of 2010, in response to Schlotzky's Deli, the very first victim that Detective Dunn responded to. And one of the first things he noticed was that IP address, 188.120.225.66. That same server is the server Detective Dunn found in the internet history for several victim systems pulling down the malware defendant used to scoop up credit card track data. But when Detective Dunn first saw it, it had been renamed, shmak.fvds.ru. Shmak is another one of defendant's go-to usernames. Not only did defendant rename the smaus server to shmak, it's the name he used for some of the early versions of his malware seen at Schlotzky's Deli.

Defendant's shmak username also shows up on other parts of the infrastructure. When Detective Dunn searched the HopOne servers, one of the first things he noticed was the username for that server, logging in from Indonesia, was also shmak. An internet history on the HopOne server tied it right back to the shmak server in Russia, as defendant was surfing his malware storage.

The shmak and smaus server, and its ties to HopOne, are the bridge between defendant's days as nCuX and the emergence of track2 and bulba. And the HopOne server brings you full circle to the rubensamvelich account. That's the e-mail account with the PayPal receipt, the one that defendant was

using to manage the HopOne server and the track2 vending sites. These are the servers and the sites that defendant opened up in 2009 and 2010, after ditching his nCuX name and taking on the persona of track2 and bulba. What do we find there, in the rubensamvelich account, but the same smaus and ochko123 password, over and over again, for personal internet accounts.

And tying it all together, in 2014, defendant's go-to username, smaus, is the username he chooses for the laptop strapped to his shoulder when he was caught on vacation in the Maldives. How many of you guessed the password for that computer? Agent Fischlin got it right on the very first try, ochko123. Of course he guessed it right. It was everywhere. It was the thread connecting defendant to all of the infrastructure throughout this case.

That signature password and the smaus username ties defendant to everything, his days as nCuX, the boookscafe account, the rubensamvelich account, the HopOne server, everything. And it ties him to this laptop with all of the incriminating evidence that Agents Mills and Fischlin found. It opened up a flood of incriminating evidence that this defendant is utterly desperate to avoid.

Mr. Blank would have you believe that all of this evidence on defendant's laptop can't be trusted; that some super-hacker planted 1.7 million credit cards and all this internet history, carding forums, pages of user credentials for defendant's

criminal infrastructure; and that this super-hacker somehow went about erasing the hundreds and hundreds, if not thousands, of internet artifacts and forensic artifacts that would have shown something like this had happened.

But Mr. Blank is an advocate. He is an attorney, paid by the defendant. Without even looking at the forensic evidence before writing his report, he claims this computer can't be trusted. Mr. Blank has sold his opinion to the highest bidder, and his testimony is contradicted by all of the evidence in this case. He's brought you absolutely nothing to support this opinion. And he wants you to ignore a mountain of forensic evidence that directly contradicts everything he said. It's based on pure speculation.

And the Court has instructed you, in Instruction Number 3, that this just doesn't cut it. Reasonable doubt is doubt based upon reason and common sense. It isn't based purely on speculation. And that's all that Mr. Blank has offered you, speculation. He wants you to ignore the security logs, ignore the event logs, ignore all the registry keys, ignore the Volume Shadow data that Mr. Carroll told you about. All of the logs, all of the databases, all of the evidence on this computer, and everything you saw before that computer, shows that nothing was wrong with this. The evidence on that computer is inherently trustworthy. And the last person to ever log on to that computer was this defendant, on July 5, 2014, right before he

was captured.

But, of course, the defendant wants you to ignore that evidence. It's the nail in his coffin. That computer is loaded with evidence of his crimes. It shows his internet history, browsing to all of these carding forums, hanging out on some of the world's most notorious carding forums, and advertising his own vending sites, 2paccc, the best dump market. It has defendant's banner ad for his newest vending site, conveniently placed on his desktop within easy reach so he could add it to any carding forum that advertises here. And it has cheat sheets with the passwords and usernames for his entire criminal enterprise, going back to his days as bulba.cc, including his Liberty Reserve account credentials, where he received the millions of dollars in proceeds, and his carding forum logins that he was using to advertise his goods.

And all of this evidence on the laptop is not only corroborated by the fingerprints and digital signatures he left throughout the crime scene over several years, it's also corroborated by the defendant's iPhone. Mr. Blank didn't say anything about the iPhone. And you've seen that, too, has the references to smaus and ochko, as well as defendant's BTC, Bitcoin, account, his preferred method of currency as 2Pac.

At the beginning of this trial, Mr. Browne told you that the world is watching. Darn right, the world is watching. This defendant has been wreaking havoc all over the world for

nearly a decade, hacking victims like Diane Cole, who had to pull out her own credit card to cover the payroll; and CJ Saretto, who had to shut down Broadway Grill and declare bankruptcy after defendant's attack on their point-of-sale system destroyed their business's reputation in the community. These were victims who thought they had done everything right, victims who thought their point-of-sale systems were secure, who had no idea that this defendant was prowling the internet at night, looking for unlocked doors he could barge through and steal from their systems.

Members of the jury, the evidence in this case supports only one conclusion. The person behind these attacks is this defendant, Roman Seleznev. His digital fingerprints and signatures scattered about the e-mail accounts, servers, and domains used to run his enterprise that he was -- show that he was the person behind the keyboard, who was acting as nCuX, track2, bulba, and 2Pac, from 2007 through the day he was arrested in 2014. He was the person running one of the world's largest credit card trafficking schemes, responsible for over $169 million of credit card losses, thousands of banks and merchants around the world.

Because all of the evidence in this case has consistently pointed to one person behind the keyboard, we ask that when you go back to the jury room, you return the only verdicts that are supported by the evidence in this case, and that is guilty on

all 40 counts charged.

Thank you.

THE COURT: Members of the jury, we'll take our morning recess at this time.

(Jury exits the courtroom)

THE COURT: Counsel for the government, anything to take up?

MR. BARBOSA: No, Your Honor.

THE COURT: Counsel for the defense?

MS. SCANLAN: No, Your Honor.

THE COURT: Just a reminder to all persons present, there are no recordings that are authorized or allowed by this Court. The only authorized person to record anything that takes place in this courtroom is the court reporter. Anyone else conducting such activity is engaging in illegal operations. So if you're doing that, you need to stop.

We'll be in recess. Fifteen minutes.

(Recess)

(Jury enters the courtroom)

THE COURT: Ladies and gentlemen, I now ask you to give your undivided attention to Ms. Emma Scanlan, as she gives her closing remarks on behalf of her client, Roman Seleznev.

Counsel, you may proceed.

MS. SCANLAN: Thank you, Your Honor.

Good morning. I just want to start by pointing out that

there seems to be a certain arrogance to the investigation and the presentation of this case. So there's a complete denial of the fact that we are standing here today in what is commonly known as real life. It's not on the internet. It's not on a computer. It's not digital. It's the things that you can see, hear, now. Everything the government has shown you is outside of where we stand right now. And this is where you have to make a decision. This is where all of the judgments occur.

Remember the woman in the photo? We keep seeing the picture of the airport. And you see Roman, and there's a woman in the photo. We didn't hear anything about anyone interviewing her. Did anybody ask her, "Hey, is Roman a prolific hacker for all the world to see, or not?" Not that we know. Why not?

We heard Agent Mills talk about Roman's ex-wife. He interviewed her. We saw a picture of her. She's not here.

And how about all these shadowy co-schemers, who are somewhere, apparently, out in the world, where are they? Who are they? Where are the things that tie us tangibly to the truth of this case?

The government has said they started investigating Roman sometime around 2010. We heard some stuff about a nickname that started in 2007. So we're talking about the federal government. We're talking about the United States Secret Service. We don't have a single picture of Roman sitting in

front of a computer. Where is it? We have all this time. You know he's in the Maldives, for example. That's not in Russia. We're not talking about extradition treaties. Why don't you go and see if he's got his computer at the pool, and you can take a picture? And that's the underlying arrogance of this case, is this idea that that's not necessary. We don't need to do that.

And so you see the diagrams. We have the track2 infrastructure diagram. We've all seen it a bunch of times. It has the shmak server. It's got HopOne, all the arrows. And then on the top left-hand corner, there's a laptop. And then Mr. Barbosa kept telling you, "This is the defendant" -- point -- "sitting behind the laptop." And everything that we're looking at is a blank screen. Here he is, sitting behind the laptop. And you're staring at a blank screen. And that's not enough. That's not enough to have somebody sit here in federal court, accused of crimes like this, that are this serious. And there's an arrogance to that that is not acceptable.

So let's talk about what we're here -- what you're here to decide. You're here to decide if the government has proved beyond a reasonable doubt that Mr. Seleznev is guilty of these charged offenses. We are not here to decide if he is track2. We're not here to decide if he's bulba. It's really important in this case to separate out all of this stuff about these

e-mail addresses and these nicknames from what it is you're actually here to do. We are here to look at these counts for each one, and make a decision.

Where do you start? At the beginning of the trial, back when the lawyers were talking to you, so it was -- who was it? It was Mr. Browne and one of these guys. There was this idea about the presumption of innocence. And everybody's heard that. We've all seen *Law & Order*. And we talk about it all the time, and it kind of becomes a concept where we all assume that we know what that means. And one of the jurors acknowledged that, actually, if you're going to work with that, that it takes an effort. It's hard to start out thinking that somebody is innocent. And it's hard to maintain that thought when you have lots of witnesses, and a whole bunch of them are federal agents, and you've got lots of exhibits.

And as they highlighted in opening, and now in closing, you have 40 counts. The fact that you have 40 counts doesn't make any one of those counts any more true. You can charge somebody with one crime, you can charge them with 40 crimes, you can charge them with 200 crimes. Each one is its own individual consideration.

Roman -- we talked about this at the beginning, with the presumption of innocence and the proof beyond a reasonable doubt, he doesn't have to prove to you that he's innocent. That's not how it works. All of these people that come in here

and tell you things for the government, that's their job. It's also their job to make sure that you can understand what it is they're asking you to convict Roman of.

So I was sitting around thinking about this yesterday, after we ended court, and I started making a chart. Here are these 40 counts. Now, what is the evidence that actually ties my client to each of these counts? And I did this exercise for probably 20 minutes. And then I crossed it all out, because I realized that that is not my job. It's also not your responsibility. If you are confused about what evidence they presented actually means he's guilty of a specific count, that can be a reasonable doubt. You don't have an obligation to go back and tie it all together for them. You don't have to go back and take these nicknames, and these e-mail addresses, and figure out what in the world they have to do with aggravated identity theft. That's not your job.

Let's talk about Detective Dunn. We've had a lot of people come in here. Detective Dunn is the one who works for the Seattle Police Department, and then also has a private job. So he was one of the first witnesses. He told you that Roman was the victim of a bombing in Morocco on April 20 of 2011, one of the victims of this incident. And he was talking to you about the bulba.cc website. And he told you that it was his understanding that Roman was very seriously injured, injured such that he was incapacitated through December of that year;

so we're talking about April to December of 2011. During that time period, Detective Dunn logged on to bulba, and he saw all of these different credit card tracks for sale. In July, there was first 40,000, and then there was a hundred thousand.

So did that make Detective Dunn wonder if he was right about who his primary suspect was? No. Instead, what he did, and what he told you he did, is that from August of 2011, right after those tracks came up, until the end of the year, he just stopped investigating. And he stopped investigating, as he said, because his primary suspect was in the hospital. Well, I would submit to you that that's not how you do it. The idea of this type of investigation is to figure out the truth, not to start with your idea of what's true, and then make it all fit on the back end.

Another example of this is Exhibit 16.12. It would be 16.12. One second.

Your Honor, may I have one moment?

THE COURT: You may.

Members of the jury, if you'd like to stand and stretch, please feel free to do so.

MS. SCANLAN: Thank you.

THE COURT: Please be seated. You may continue.

MS. SCANLAN: Okay. This is one of these exhibits that you will have back in the jury room. So this is Summary Exhibit 16.12. It's one of the government's exhibits.

Now, this is more than just this one page. It's this list of all the businesses Detective Dunn said were sending credit card data to the HopOne server. But when we asked him about this, did you -- I mean, "Where are you getting this? Did you verify this?" He said he verified 20 of them. So we have 600 businesses that are alleged here on this exhibit, 20 of which are verified. And it's kind of a continuing theme. There are other things in this case that I think -- I submit should give you pause. There are things that are neon signs pointing to Roman, that maybe they're just a little too bright.

So you have Exhibit 5.14; okay? So this is the e-mail where -- he -- whoever, the boookscafe guy, is saying -- at the top, it's highlighted, "I use it for illegal purposes."

Okay. If you're one of the most prolific hackers in the world, and you're super-sophisticated, are you really sending e-mails to outside companies saying, "Hello, I'm doing something illegal"? I don't know. But I'll tell you, they don't know either. Because I haven't heard anybody who went and investigated, or talked to this Christopher person, who's corresponding, supposedly, with Roman, "Hey, Christopher, are you a real person? Is this a real e-mail?" No. We're relying so totally on the digital evidence that it seems there's no need to actually go and figure out if some of this stuff is true.

And we have the same thing with Exhibit 5.6. This is the

flower order receipt. Mr. Barbosa was just talking to you about this one too.

Okay. We have a receipt that says flowers were sent to Svetlana, who is Roman's ex-wife. Well, this is the company name, right, "sendflowers.ru." Who verified that? Who even tried to check and see if this is a flower company, or if this is a receipt? Did we ask this company, "Did you send flowers on that day to anyone?" No. But why not? This isn't an investigation that happened in 30 days. As they keep stressing, this is an investigation that occurred over four, five, six years. No one felt the need to verify any of this information.

And it's the same thing with the posdumps website. So you just saw that a couple minutes ago. And Mr. Barbosa was telling you how remarkable it is that it says on there, "Remember, this is the illegal way." Well, something just isn't fitting here. So is he a sophisticated hacker, or is he a total idiot, frankly? Is he creating things and then just saying, right there, on the internet, that they're illegal? I would submit to you you can't have it both ways. Is it one or is it the other? So is this his, or is it not? I don't know.

The other thing about what Detective Dunn told you is that he told you that back to when Roman was injured, that time period, that he was still communicating with somebody at bulba.cc. He was asked by the government who that was. And he

said there were two parties, admin and support. Well, as far as I recall -- and trust your collective memories over mine -- but my recollection is that the government keeps saying that Roman is admin. So how is Detective Dunn talking to Roman when he's saying that Roman is unavailable? And who's going to explain that?

How about the IP address for shmak or smaus, whatever it's called? So in that diagram, it's the one that they keep telling you the malware came from to all these businesses. Detective Dunn told you that he went on the internet, he got on the server, he downloaded the malware, and it worked just fine. So if this was malware that belonged to Roman, and it was just his, it was just this group's, why is it so openly available? Why isn't it protected by even a basic username and password? We saw multiple websites in this case with username and password login screens. But this malware, that's supposedly such a signature for this individual, is just readily available. You can just go and get it.

And I think part of what the government would tell you, perhaps, is that this is the shadowy co-schemers; right? This is all the people that we have no idea who they are. And they're using it too, and so that makes him responsible for it. But we have -- who are these people? How can you ask to hold someone responsible for something when you really have no idea who they're saying did what, when?

You have an instruction, Instruction Number 21. Instruction Number 21 is about this whole concept of the scheme to defraud. So these are all the co-schemers, whoever they may be.

First, you have to decide -- at the outset of this instruction that the judge has given you, you have to decide first, before you start holding Roman responsible for what these unnamed people did, you have to decide that he's a part of a scheme with them. I would submit to you that you don't have enough information right now to make that decision. There's been a lot of speculation, there's been a lot of guesses, about what the connection between Roman and these unnamed people is. But the speculation of who it could be and who it might be isn't in evidence. There's no scheme that's been proven here.

So Instruction 28 is kind of a similar situation. This is what we would call an instruction on aiding and abetting. So it's very similar to the scheme to defraud instruction, and it's really the same issue.

This instruction is telling you that Roman can be responsible for what other people did. I would draw your attention to what starts on Line 16. The line numbers are over on the left. It's not enough the defendant merely associated with the person committing the crime, or unknowingly or unintentionally did things that were helpful to that person, or

was present at the scene of the crime. The evidence must show beyond a reasonable doubt that the defendant acted with the knowledge and intention of helping that person commit these offenses.

So just because you can link Roman to a website, and you know that people on that website were doing a bad thing, that's not aiding and abetting. Showing an association, without more, is not a crime. You have to show what specifically this person did; not just was he on the website, what did he do that aided and abetted these other people?

And we don't know what he did or didn't do at this point. We know he -- I'll give it to you. He's associated with all of these things, with these websites and the HopOne server. They've clearly shown these kind of paths of association. It's not the same thing as committing a crime. So you have to be -- that's part of what's difficult here. You have to be careful in this case. Because you can show that somebody hangs out with bad people, or goes on bad websites. That doesn't mean they transmitted malware on a particular day to the Broadway Grill. We have to separate those two things out and focus on what he is charged with.

And speaking of the Broadway Grill, so the Broadway Grill, Detective Dunn told you there was 32,000 credit card numbers that were in a text file. This text file was exfiltrated, or taken away from, the Broadway Grill's server, and sent

somewhere else by someone who was not allowed to be in that system. Where did it go? It went to a website called SendSpace. When you look at your diagram they've been showing you, it's not on there. There was absolutely no connection, whether association or not, between Roman and SendSpace. So when they ask you to convict Roman of taking that and doing that, that should give you pause. It's not that easy.

So the government -- it makes a lot of easy sense to say all of this starts with the wire fraud counts. If you look at these, then it's like dominoes. All these other things are true, all the way down the line, all of these 40 counts. But, no. They're each individual decisions. So you have to decide if that's enough to tie Roman to somebody sending credit card numbers to SendSpace, or not. There's no domino effect here. Each one is an individual decision.

Agent Szydlik, he was one of the agents that came from Washington, D.C. So he talked to you a little bit about the same sort of speculative co-schemers.

So if we look at Exhibit 10.3, now this -- you'll have this, so I'm not going to make you read this. This is another one of those things that's really not explained. So the government has said that Roman is 2Pac. Roman was arrested on July 5 of 2014. On July 21 of 2014, the agent told you, 2Pac logs on to the carding forum verify.ru.

And he also told you that these nics -- so 2Pac is a

nickname, or "nic" -- are very valuable. I think an analogy for the value of that, for instance, would be that Microsoft calls their operating system "Windows." You can't open a computer company and name your operating system "Windows," because that's their name, and they've built it as a brand, and people trust it because of that branding. And they've drawn that analogy for these nics. 2Pac is a name that, apparently, had weight in this particular community. So it's not a name that you can just adopt willy-nilly. But here it is.

So Roman -- no one disputes that Roman has no access to a computer at that point. But here's 2Pac. Now, the explanation for this has been that there are co-schemers. Who? Who are the co-schemers, and where are they? I don't know. So you can speculate that it's a co-schemer. You could also think that perhaps it's just not Roman. But either way, you don't know. We don't know what the answer is to that. And these are the types of things that should give you pause when you look at this case.

And it's the same thing -- we talked to that agent a little bit about IP addresses, in general. So he said, quite honestly, that an IP address can connect to a particular computer or an entire network of computers. We talked to him about internet cafes. So if I sit down in an internet cafe, on a computer, and I get up, Mr. Barbosa sits down right after me, he gets up, you can't tell which one of us did what, just the

fact that we were at the same IP address.

That's another issue. An IP address is not a digital fingerprint. An IP address is a location of a computer or an entire network. That's why it might have been important to actually connect Roman to a keyboard. That's why it is important to recognize that when we say Roman is at that keyboard, what we're looking at is a blank screen. Because an IP address is really not enough to identify an individual person.

Let's talk about Mr. Fischlin in the context of the Red Pepper Pizzeria. So there's so many agents -- he's the agent who came here, who recently left the Secret Service and went to the postal inspection office. He's the one who went to Red Pepper Pizzeria, to the guy's garage, and took the servers and looked at those. So that is Counts 11, 20, 29, 38, and 40.

Mr. Barbosa mentioned, and I think he's correct, that the defense position is that there was no evidence that Roman had anything to do with taking the credit card numbers off of that server. So Mr. Fischlin came here, and he told you that the malware that was installed in the Red Pepper Pizzeria system is called Perfect Keylogger. It's not called kameo, or dtca, or dtca2, or any of those. It's something called Perfect Keylogger. He also told you that that malware is commercially available. So in other words, you can just buy it. That's the malware that was seen on the Red Pepper Pizzeria system. Then

somehow the credit card numbers got off of that system and went to wherever they were going. And he acknowledged that he can't say how that happened. Well, if he can't tell you how that happened, then I would submit you can't really convict Roman of doing that.

Now, Mr. Barbosa said, "Sure you can, because there's credit card numbers on the HopOne server." Well, that's proof that there's credit card numbers on the HopOne server. Yep. I agree with that. That is not evidence -- again, separating out the counts -- that someone took credit cards off of Red Pepper Pizzeria's system and sent them somewhere.

So when you look at all these counts by the victim business, make sure you separate it out, please, exactly what is alleged in each count to have happened. Because there's different varying things going on here, in terms of what proves each of these charges.

Megan Woods [sic]. Megan Woods was the data analyst from the Secret Service. So Ms. Woods does not appear to be an accountant. So I'm going to acknowledge that. But -- so she took, at the instruction of someone else, I'm sure, all of these credit card numbers that the agents and the detectives sent her, and she sent them all to Visa and MasterCard and Discover and AmEx, and they sent back a bunch of information. And then there was a decision made about what financial institutions that went with. But she told you, no one verified

any of that.

So Mr. Barbosa is talking about these 3,300 financial institutions. Well, maybe. No one has verified any of that information. And the excuse for that was that there isn't time. There hasn't been time in the last four years, before you accuse somebody of 1.7 -- or however -- $170 million in loss, of perhaps verifying the accuracy of that information.

Or how about the credit card account holders themselves? There was kind of an insinuation that it's ridiculous that somebody could try to contact all those people. Okay. How about a sampling of them? How about you call 100 of them? "Hey, I see that there's a credit card transaction here with your name on it. Is this a fraudulent transaction? Did this happen to you?" That's not beyond the pale of what we should expect from our federal law enforcement.

Okay. Counts 12 through 20 are the intentional damage to a protected computer. So, first of all, you might want to ask yourself if these are protected computers. So what we've heard from everyone is that these computers have vulnerabilities. And it's not -- I'm not blaming Mr. Saretto, or the Casa Mia owner for this. That's not what we're here to do. What I'm saying is that their systems were vulnerable. They weren't up to code for what -- the protections they needed to have to take these credit cards.

And all of those fines -- and when you're asked to find

this $5,000 or more for each of them, they were fined this money, not because somebody took their credit cards, but because their systems weren't compliant. I am certainly not saying that what happened to them is fair or deserved because of that. Nobody is going to stand here and tell you that. I am saying that before you convict somebody for a certain sum of money, you need to decide why those fines were assessed. And were they assessed because somebody took credit card numbers, or were they assessed because these businesses aren't compliant? It's a decision that you need to make. But I would submit to you that really what we know is that they had vulnerabilities; and that because this happened, they had to fix them.

The last major thing I want to talk to you about is the laptop. So I would guess that some of you have been wondering why we keep going on and on and on about the laptop. And it's because, when you're the person sitting in that chair, you have a right to expect that the people who are making you sit there are doing their jobs correctly. It's not nitpicking to say that you should handle electronic evidence in the correct way. But it didn't happen here.

So we all heard about the dual missions of the Secret Service, I think four or five times. So we have the mission of protection. So they protect executives, et cetera, the executive branch, the President. Then we have essentially

cybercrimes. That is one of their two specialties. So when we go through and we perhaps criticize what they did in this case, let's keep in mind that we're not criticizing a small, local police department. I'm not expecting that the police department in Duvall use a Faraday enclosure, in 2014, to seize a laptop. What we are expecting is that the United States Secret Service, who specializes in these types of offenses, would do this correctly.

Agent Iacovetti seemed like a nice guy. He's the one who came here. He was sent to the Maldives to get Roman and get all of Roman's stuff. He didn't bring a Faraday enclosure. He didn't bring one for the laptop. He also told you he didn't bring one for the iPhone. Now, the Faraday enclosure issue is not limited to what Mr. Blank says. Detective Dunn told you that that is a regular course of business thing that one uses. They didn't turn it off. They also didn't plug it in.

So Agent Mills gets the laptop over here in Seattle, with Fischlin. And they are looking for the serial number for the third time, for some reason, and it comes on. And they tell you that they're worried about encryption. Okay. They're worried about encryption. So we heard multiple people describe what you do. If you're worried a computer is encrypted, then you want to make this image or copy of its drive before it turns off. But they both told you it turned on. It was in the vault, the vault that they hadn't signed in and out of, and

they just left it there for 23 days.

So these live images, this is not rocket science, in 2014, in this field. These live images need to be done quickly to be accurate. Why? Because you are putting people on trial based on what is on these computers. It's important. It's like preserving a crime scene with the tape, same idea. And it's just as important as that concept. But they just left it there. And in the meantime, all of these things happened.

Now, we say that's important, because it affects the integrity of the investigation. Detective Dunn tells you that any changes to a computer drive before you image it, he -- those are his words -- affects the integrity of the investigation.

Now, Mr. Carroll tells you, "Don't worry. There's nothing wrong with this computer. Doesn't matter that they did this, because I can tell you definitively that there's nothing wrong with it." Well, Mr. Carroll works for the Department of Justice; and so do they. And they have an opinion, a vested opinion, about this computer and how it was handled. And I would -- I wonder why the government keeps saying that Mr. Blank's opinion is that somebody imported all these files, because Mr. Blank kept repeatedly telling you that he doesn't know. The point of his testimony is that we have no idea what was going on here.

We know there's a SIM card. As of June, we know this. We

know that it has this connectivity capability. We know -- and Mr. Carroll says the log says there was nothing connected. We also know these logs can be edited. So essentially, we have, right now, a whole bunch of confusing information about what happened to this laptop, and a whole bunch of people with different opinions.

And this is where it's important to remember whose responsibility it is to make this make sense for you. Because it's not Roman's. If that's a piece of evidence, and it's handled in this way, then you need to decide if that handling alone is enough to give you pause; if it's enough to make you wonder why in the world they gave this laptop to an agent who, at that point, had done less than 40 forensic examinations? This is the Secret Service. Fischlin had done over 500; Szydlik and the entire department he comes from in Washington D.C., probably thousands. But for some reason, this decision is made to give this laptop to essentially this poor guy, who really doesn't have the experience to be doing this. He's never, at this point, seen a computer with Windows 8. There's been no dispute that Windows 8 had been out for a couple of years before all of this went down. It's not his fault that he hadn't seen it, but it is the fault of this investigation that he is put in that position. And it's not something that you can rely on.

One more thing before we sum it all up and I'm done. The

last two counts, 39 and 40, which are the aggravated identity theft, where are those people? So one of the things they need to prove is that they're real people. But they didn't come here. So on a basic level, you know, they identify who they are, we know their names, but they're not here at the trial. So is that enough to show that -- if you even assume that Roman did this, is that enough to show that he knows it's a real person, when we don't even know? It's not. So those two are kind of the separate, outlier issue.

Essentially, what we have is an investigation and a presentation that is really built on the arrogance of digital evidence. And that's not enough. It's not good enough when you ask somebody to stand trial for charges like this.

At the end of the day, I ask you to consider everything really carefully. I know that you will. There's a massive amount of information. But the decision that you make is final. So take your time. If you make a decision, and you decide tomorrow that maybe, you know, it does matter that the thing sat there for 23 days, you don't get to change your mind. This is it.

And I would submit to you that at this point, with what we know, and with essentially a blank screen sitting behind this computer, we don't know enough to be confident beyond a reasonable doubt that Roman is guilty of these charges. And if we don't know, or we're confused, or we don't necessarily see

the connection between some of the counts and all of these nicknames, then the thing to do is to find him not guilty.

Thank you.

THE COURT: Members of the jury, if you'd like to stand and stretch, this is an opportunity to do so.

Ladies and gentlemen of the jury, the government carries the burden of proof in this case. And because of that, they have the opportunity to respond to the defense arguments by way of what's called "rebuttal argument." I now invite you to give your undivided attention to Mr. Harold Chun, as he gives his rebuttal argument on behalf of the United States.

Counsel, you may proceed.

MR. CHUN: Thank you, Your Honor.

American Express, they should be proud. Because the defendant took, "Don't leave home without it," to the next level, carrying 1.7 million credit cards in his laptop as he travels. I could see why he wants to shy away from that computer. But it's his, taken from him, from his laptop bag. You saw that. But I'll come back to the laptop.

First, let's talk about how Ms. Scanlan started her argument: No picture in front of the computer, him sitting in Vladivostok, Russia, typing on his computer. The government doesn't have it. We agree. The government doesn't have it. But you know what we do have? Showing you what's been marked as Government Exhibit 14.5. We have a photo that the defendant

took of his own screen, as he chats, as 2Pac, about carding, taken from his iPhone, seized from him.

Mr. Blank didn't testify about the iPhone, on the iPhone. You know how else we know that's his iPhone? Because on that same phone was a picture of his passport and a picture of him taking selfies with that phone, the one there, and another one there. Same phone, him, holding it, taking a photo. On that same phone, him, typing, as 2Pac. That's a picture of him on his computer.

Now, Ms. Scanlan talks about association, co-schemers. How do we know he's working with someone? Well, the evidence has borne it out. We have seen throughout this case that he is working with other people.

Starting with Exhibit 2.13, Ms. Scanlan said, "Well, the website was still up after the bombing." Well, let's be clear. What does this show? It says, well, the admin is saying you need to wait. They don't have numbers at that point.

Then moving on to Exhibit 10.3, after his arrest, what happens? The boss, in a car accident. Someone working? But you know who's here? The boss, sitting right there.

And how else do we know he has people working with him? 6.13, Page 3, as he e-mails on this infrastructure as Romper Stomper, he tells them, "I have a high-skilled administrator." He's telling other people he has people working for him, but he's the boss.

Now, I'm not even going to entertain, actually, the argument that did -- Detective Dunn didn't call all the hundreds of businesses, because it's laughable in the same sense that -- defense crossing about not calling all near three million customers. Is that what the government needed to do to prove this case?

And the defendant saying, "This is the illegal way," in an e-mail, he wouldn't be too clever to do that? Well, obviously he doesn't care, because he puts it on posdumps, which is a website for the public, to teach them about how to buy credit cards and use them for fraud. And he taglines it, "This is the illegal way." He wants people to know.

And this talk about not having follow up for flower receipts from a flower shop in Russia, what would you find in contacting a flower shop in Russia, other than the receipt, which is already in the e-mail account tied to this case? Flowers were sent, under a name that they would record it. An online purchase would have an online receipt.

And that brings me to Broadway Grill. You heard the agent testify that SendSpace was used to exfiltrate this data. Well, if you look at the timing of when that occurs, it times up perfectly when that intrusion occurs. You know that somebody hacks into this machine, downloads their malware. And at the same time, they find a stash of 30,000 credit cards in the clear, and they export it right out. You don't need to know

who SpendSpace was. It's a website. But they used SendSpace to take it out.

Red Pepper Pizza. Defense counsel mentions, "How do you know the credit cards from Red Pepper Pizza were taken by him?" Well, you know just from the malware, the secretly hidden malware with the password 2pacsakur. That's him. But if that's not enough, Agent Fischlin told you Ruth Gebhard, the victim, Count 40, who he talked to, a real person, said -- or Agent Fischlin said that card was taken from Red Pepper Pizza. Where is it found again? On defendant's laptop. Examine the evidence. Common sense tells you how it got from Point A to Point B. It's because he took it.

And this belief or attempt to blame the victims for not protecting their systems, and therefore, you know, they almost had it coming to them, or, you know, that's why they were fined. I think it was best summed up, actually, by Mr. Doyle, when asked by Mr. Browne, wasn't it basically his fault. He said, "No. It's because I got hacked." That's not what he signed up for.

And that brings me to the computer, the laptop. You heard a lot of testimony yesterday about the integrity of this laptop. And first you heard from the forensic examiner for the defense, their forensic advocate, the same forensic examiner who said he wrote his forensic report without reviewing the forensics on the computer. Let me say that again. He wrote

his report without examining the forensics on the laptop. That's like writing a book report without reading the book first. That's what he did.

And then what did he tell you that report said? Well, he said it's a possibility that the agent mishandled evidence. It's a possibility that some unknown person remotely logged on and planted evidence. Possibilities, theories, that's what Mr. Blank had. In short, he had pure speculation. That's what he had. The only thing he was certain about, the fact that he couldn't recognize the forensic exhibit shown to him on the stand, and that he couldn't tell you if any of the government's trial exhibits were affected by this at all. He didn't know. That, we know for certain.

And then you heard from Mr. Carroll, who took the stand. And what he told you was, he examined that computer thoroughly. And what he found was that it was reliable, and that he found no issues with its integrity. And then he didn't just offer that opinion. He showed you exhibit after exhibit, artifact after artifact, proving consistently across the operating system, nobody's ever logged into this computer after the defendant was arrested, and the computer never connected to any network wi-fi or cellular after the defendant was arrested. Those are the artifacts he showed you.

And in regards to the file dates changing, the access dates, he told you, while that computer was sitting in a Secret

Service vault, awaiting the case agent to get a search warrant, the case agent who was in Seattle and had to fly to Guam for a court hearing, the computer did what computers do, routine system stuff. Antivirus ran. Windows update ran. Program updates ran on its own.

Mr. Carroll didn't stop there. He then told you that he examined the government's trial exhibits and found exactly one file that had an access date after the defendant's arrest. And he told you it wasn't a created date. It wasn't a modified date. It was an access date. And he said access dates aren't routinely used by forensic examiners, because too many factors can make them change.

But he didn't even stop there. He then went on to tell you, that one exhibit, the 2Pac banner from the laptop, he was able to reach into a Shadow Volume Copy on that computer and archive from a prior date before defendant's arrest, when the laptop was in his possession; and from that archive, he pulled out that file, compared it to the government's trial exhibit, and he said they were identical. That's computer forensics.

And that brings me to my last point. We talk about the laptop, and that might be fresh in your memory, because it just happened yesterday. But this trial has been going on for days and days. And you have heard evidence prior to Mr. Blank's speculation about the laptop. And the question is, did anyone have a doubt that HopOne, the Ukraine server, shmak.fvds,

bulbacc, track2.name, romariogro, rubensamvelich, that all of these weren't controlled by him? No. The evidence from all of these places match up. You saw smaus. You saw ochko. You saw IP address after IP address connect. It wasn't just one cafe and another cafe. You had an IP address from Indonesia, all the way out to McLean, Virginia, touching e-mail addresses, servers, all parts of the infrastructure. That's a common web. That's not coincidence. It's because it's the defendant connecting to those sites.

What else did you see? You saw his name. You saw his date of birth. You saw his Vladivostok addresses. You saw his telephone number. You saw his passport ID. These things kept popping up over and over again on different pieces of that infrastructure. All of that, evidence collected from different servers, from different e-mail addresses, over different years, spanning years of time, they all matched up. And that's what led to his arrest when he was in the Maldives. That's what led there, the Secret Service to him there.

And what did they find when they got there? They found his actual passport, with the number that matched the Western Union records, that matched the travel records found in HopOne. They found his iPhone, littered with evidence of smaus, ochko, romariogro.

And his statement upon being confronted by law enforcement, he asked the question, "Does the United States

have an extradition treaty with the Maldives?" Who asks that? He did. That's what he asked.

And then that brings us back to the laptop; 1.7 million credit card numbers; a script of posdumps on it that says, "This is illegal way"; federal court record searches for his nicknames, bulba, 2Pac; and his password credential list.

His password credential list, Exhibit 13.12C, Page 13, that credential list connecting him to criminal forums, connecting him to Liberty Reserve accounts, and connecting him to an identity he long abandoned, bulba; bulbacc@yahoo.com and the password, sitting right there on that credential list; right below that, the Liberty Reserve account you heard testimony about, ending in 915; the Liberty Reserve account that received almost $7 million from the bulbacc website; and then right above that, bringing it right back to the present time, just a few lines above, 2Pac, the site he was running at the time he was arrested.

Ladies and gentlemen, to be clear, that laptop, that was just frosting on the cake. The evidence before it all had built it up to that point. And everything after that, at his arrest, that laptop, that just coated it. And the cherry on top, the password for it was ochko123. You can't make stuff like that up.

Ladies and gentlemen, go examine all the evidence, and return the only verdict that is consistent with it all, guilty

of all counts.

Thank you.

THE COURT: Ladies and gentlemen of the jury, at this point in time, as the Court shared with you at the beginning of the trial, only 12 of you go back and actually deliberate. And so we must now separate two of you.

Now, when you came to the court, you were summoned by a computer, so you came in a random fashion. When you were brought to this courtroom, the order in which you were selected to come to the courtroom was done by computer. But at this point in time, we go back to the old, traditional way of selecting jurors to serve as the alternates. And that's to go back to the old jury box, where we have numbers in that box, and we'll pull two numbers. And the order in which you're selected will be the order in which you might be called back to serve as substitute or alternate jurors. So I'd ask the in-court deputy, at this point in time, to identify the jurors who will serve as the alternates.

THE CLERK: Juror Number 8.

THE COURT: Number 8.

THE CLERK: And Juror Number 15.

THE COURT: All right. You can stay in place for right now.

For the two jurors that are excused, the following instruction will apply to you. You will still be a member of

this jury. Although you will be separated from the jury for purposes of the deliberations, you may be subject to recall if for any reason one of the other jurors is unable to continue to go forward in their service as a juror. So in that regard, the same restriction and direction that you received from me in the past about not discussing the case with anyone, not sharing with anyone your thoughts about the case, and certainly not giving anyone any information how you would have voted or deliberated in this case. So the prohibitions on silence for you talking about this case will continue. If you're called back, you will be called back in the order in which the Court announced. So please make sure that when you leave, you leave the in-court deputy with all numbers to be in contact with you.

I will let you know that it's my understanding that the jury will be taking lunch in the jury room, so that they won't be separated and walking around and enjoying lunch between 12:00 and 1:30. They'll be back in the jury room. So we need to have your access information for that time period. Their breaks will also be taken in the jury room. They will not be separated until 4:30, at which time they would break for the evening. As I shared with you at the beginning of the trial, we don't deliberate into the late evening hours. We stop at 4:30 and begin again at 9:00, with the same expectations to continue until the jury has made determinations in this case.

So for the two jurors, I do want to thank you deeply for

your service. I want to thank you for returning to this court every single day, and for your attention and the service that you provide and that you granted as jurors. It's what we expect of our jurors, and you fulfilled your responsibility up to this point in time.

To the other members of the jury, you'll go back and begin your deliberations. I will also let you know that all of the admitted exhibits will come back to the jury room. And just to make sure that you understand what I mentioned before, if the exhibit was marked for identification, or if it was a demonstrative or an aid for a witness, those type of exhibits will not come back to the jury room. Only those offered and admitted by the Court will come back.

Please rise and go back to the jury room and begin your deliberations.

(Jury exits the courtroom)

THE COURT: Counsel, we're going to take our break at this point in time. I've already identified what we're going to do as far as the jury over the lunch hour.

I do ask that you make sure that all of you have your contact numbers provided to the in-court deputy. That's cell numbers, direct lines at work, so that if we need to reach you, we can reach you. And we expect you to return back to this court 15 to 20 minutes after a call from this court.

Now, if we do have jury questions, it's never been my

practice to play hide-the-ball from the lawyers. If we receive a question from the jury, the in-court deputy will contact you and read the question to you over the telephone so that you can begin formulating your response to the jury question, and make your recommendations in open court. That will always take place.

For Mr. Seleznev, any questions or anything that takes place while this case is pending will always be done in open court. I will not consult with the lawyers in this case without you being present. So if there's a jury question, although we read the jury question to the lawyers over the phone, that question will not be answered until everyone is back in this courtroom, including yourself.

So with that, Counsel, please make sure that we can get in contact with you so that we can reach you at the appropriate time.

Anything to take up? Mr. Browne?

MR. BROWNE: Just one question, your Honor. When we were going through the exhibits yesterday, I noticed that there are two or three DVDs.

If -- does the jury have the ability to look at those in the jury room, or would you bring them in here to do that, if they wanted to see it?

THE COURT: It's the latter, Counsel. This Court never sends any equipment back to the jury room. So if there's

a desire or need to view any exhibits in that format or fashion, we would bring them back into the courtroom. I suspect that they would ask what they would like to look at, and we can play the entirety of the DVD, or whatever portion is appropriate or necessary. But it will be done in open court. No equipment will go back.

MR. BROWNE: Would you want us there for that?

THE COURT: Absolutely, Counsel. You'd be coming back. Again, nothing will take place without the parties' and Mr. Seleznev's presence.

Any other questions or matters to take up, counsel for the government?

MR. BARBOSA: No, Your Honor. Thank you.

THE COURT: Counsel for the defense?

MR. BROWNE: No, Your Honor.

THE COURT: We'll be in recess.

(Adjourned)

(End of requested transcript)

* * *

I certify that the foregoing is a correct transcript from the record of proceedings in the above matter.

Date: 8/24/16 /s/ Andrea Ramirez

Signature of Court Reporter